

Microsoft Outlook 2000 Service Release 1



White Paper

Contents

Executive Summary.....	3
Overview.....	4
CMS and S/MIME Standards for Secure E-mail Messages.....	4
Simple Upgrade Path.....	5
New Security Features in Outlook 2000 SR-1.....	5
Enhanced Secure E-mail Messaging.....	5
Diffie-Hellman key agreement for encryption.....	5
Dual key support for encryption and digital signing.....	6
Secure receipts.....	6
Security labels.....	6
Multiple layers and multiple digital signatures per layer.....	6
Simplified Interface for Secure E-mail Communications.....	6
LDAP support in-the-box.....	6
Automatic settings configuration.....	6
Security properties in Contacts.....	7
Signed By field on Read Note form.....	7
Default security settings added to Global Address List.....	7
Enabling Outlook 2000 SR-1 Features.....	7
Configuring Outlook 2000 SR-1 Features.....	8
Additional Information.....	10

Microsoft Outlook 2000 Service Release 1

White Paper

Microsoft Corporation

Published: March 2000

For more information, please see <http://microsoft/office/ork>

Executive Summary

The Microsoft Outlook® 2000 Service Release 1 (SR-1), included in the Microsoft Office 2000 SR-1 release, is an update to Outlook 2000 that provides support for the Secure/Multipurpose Internet Mail Extensions (S/MIME) v3 standard. The new release includes enhanced encryption and security features such as security labels and signed receipts. These new features support the S/MIME v3 protocol, an Internet standard that extends S/MIME v2. (Outlook Express and Outlook 98 implemented most of S/MIME v2 requirements.)

Note The features in Outlook 2000 SR-1 that enhance secure e-mail messaging require Microsoft Windows® 2000. New features that provide a simplified user interface for secure messaging do not require Windows 2000.

This update is of special interest to organizations that have internal requirements for S/MIME v3 support. For example, this support is a core requirement of the U.S. Government Medium Assurance Messaging standard.

Outlook 2000 SR-1 security and encryption features are installed with Office 2000 SR-1, but they are visible and enabled only when you add a subkey to the Windows registry and set its value appropriately. If you do not set the value in the new subkey, then Outlook 2000 SR-1 maintains the user interface and feature set of Outlook 2000, and you cannot see the new features.

The following security and encryption enhancements are included in this update and described in detail later in this document:

- The Diffie-Hellman key agreement standard, which is used for message encryption.
- The Digital Signature Standard (DSS), which provides dual key support, allowing separate keys for encrypting and for signing e-mail messages.
- Secure receipts and security labels.
- Multiple layers of encryption and signatures and multiple digital signatures per layer.

Outlook 2000 SR-1 also provides new capabilities that help users more easily access and use these security features, including the following:

- Access to certificates on a Lightweight Directory Access Protocol (LDAP) server.
- Automatic configuration of settings for security profiles.
- Security properties in Contacts to control encryption to external addresses and let users share Contact entries that contain certificates.
- **Signed By** field on the **Read Note** form.
- Ability to add default security settings to the Global Address List.

Overview

Outlook 2000 Service Release 1 updates Outlook 2000 with capabilities that meet all requirements of the Defense Messaging System used by the High Assurance Message community in the U.S. Government. This update is accomplished by bringing together features from the following three e-mail security standards:

- Cryptographic Message Syntax (CMS)
- S/MIME v3
- S/MIME v3 Extended Security Services (ESS)

CMS and S/MIME standards for secure e-mail messages

CMS is an Internet draft standard that defines the structure of secure e-mail messages. CMS is based on the Rivest-Shamir-Adelman (RSA) public key cryptography standard (PKCS)#7 message format, but CMS extends the data types and semantics around it.

Primary distinctions between CMS and PKCS#7 include the following:

- CMS allows message bodies to be nested without intervening MIME headers. This capability supports triple-wrapped messages and also enables multiple security label and gateway encryption.
- With CMS, **RFC822 From** properties are not required to match the certificate subject or alternate subject names of the signed data.
- CMS explicitly supports and prefers DSS and Diffie-Hellman key agreement instead of RSA-based algorithms. CMS provides support for Key Agreement and Key Encipherment in addition to Key Transport protocols.
- CMS adds unprotected attributes as part of the EnvelopedData structure to carry additional information outside of an encryption layer.

Outlook 2000 SR-1 enhances secure messaging following the CMS and S/MIME standard. These enhancements include:

- Support for sending and receiving messages with the following content types: SignedData, EnvelopedData, and Data.
- Support for receiving messages with arbitrary nesting of CMS content types.
- Ability to validate digital signatures within arbitrarily nested CMS messages.
- Ability to use Ephemeral-Static Diffie-Hellman (ESDH) key agreement algorithm and key agreement protocol.
- Ability to use DSA signature algorithm, if support is available on the Exchange Key Management Service (KMS) Server.

Simple upgrade path

Installing the Outlook 2000 SR-1 is a simple upgrade for administrators, regardless of whether you enable the new Outlook features. No new components or Setup changes are required when you install Outlook 2000 SR-1 or customize your installation by applying a transform. The user interface and feature set of Outlook 2000 are maintained during the upgrade unless you decide to enable the new features by way of the Windows registry setting.

In addition, Outlook continues to work with Internet Explorer 4.x and Internet Explorer 5 without the new features. There is no need to upgrade to a new operating system or a new version of Exchange Server unless you need the new features. (Note that the new security and encryption features are disabled but visible if Outlook 2000 SR-1 is installed without upgrading the operating system to Windows 2000.)

Important If you install the full Outlook 2000 SR-1 product, the new security features are installed automatically. However, if you apply the Outlook 2000 SR-1 update to an existing Outlook 2000 installation, you need to take an extra step to enable the security features. On the SR-1 CD-ROM, open the Support folder. If your organization uses 128-bit encryption, run Out128.exe. If you use 40-bit encryption, run Out40.exe.

New Security Features in Outlook 2000 SR-1

A number of features in Outlook 2000 SR-1 can be enabled to support enhanced secure e-mail messaging. Additional enhancements improve usability for these features.

Enhanced secure e-mail messaging

The following new Outlook features are provided to support S/MIME v3.

Diffie-Hellman key agreement for encryption

Outlook 2000 SR-1 supports Diffie-Hellman key agreement when encrypting messages, conforming to the CMS standard. This feature requires Windows 2000.

Dual key support for encryption and digital signing

DSS provides for separate encryption and digital signature keys. This separation allows users to have private digital signature keys while administrators provide message encryption keys, making it more difficult for an administrator to impersonate another user by sending an e-mail message signed as that person.

Secure receipts

You can send messages with secure receipt requests to verify that the recipient is validating your digital signature. When the message is received and saved (even if it is not yet read) and your signature is verified, a receipt is returned to your Inbox. If your signature is not verified, no receipt is sent.

Security labels

A security label lets you add information to the message header about the sensitivity of the message content. The label can also restrict which recipients can open, forward, or send the message. You define one or more security policies for your organization and implement them programmatically. For example, an Internal Use Only label might be implemented as a security label to apply to mail that should not be sent or forwarded outside of your company.

Multiple layers and multiple digital signatures per layer

Outlook 2000 SR-1 allows multiple layers of encryption and signatures. Together with multiple digital signatures per layer, the multiple layers support security labels and secure receipts. You can use Windows registry settings to specify error management for the multiple layers. For example, you can specify that a missing Certificate Revocation List (CRL) be considered an error instead of a warning. (The registry settings are described in "Configuring Outlook 2000 SR-1 Features," later in this document.)

Simplified interface for secure e-mail communications

The following Outlook 2000 SR-1 features make it easier to discover and use secure e-mail messages with digital certificates and encryption.

LDAP support in the box

Lightweight Directory Access Protocol (LDAP) is an Internet protocol that allows a user to find other e-mail users on the Internet or your organization's intranet. LDAP is the primary means of searching global directories that are available on the Internet. Outlook 2000 SR-1 fully supports LDAP, including specification of multiple LDAP Internet information accounts, so you can now download certificates from an LDAP server.

Automatic settings configuration

With automatic configuration of security profiles, users can discover features more easily, and administrators need not reconfigure settings when a certificate state changes or settings are updated. For example, when users add digital signatures or encrypt messages, Outlook searches for suitable certificates. Users are prompted as needed to repair broken security settings, such as a missing or expired certificate.

Security properties in Contacts

Entries in Contacts now have properties to store security and certificates information. Previously, a contact might include a pointer to a certificate stored in the Windows registry. Now the certificate is stored both in the Windows registry and in a Contact property. This arrangement allows you to forward a contact to someone else and the contact will be fully configured when it arrives, ready for the recipient to send encrypted mail to that contact. You can also create a shared folder that contains contacts to which users can send secure mail.

Signed By field on Read Note form

The new attribute **Signed By** on the **Read Note** form lists all subject names from the **SignerInfo** properties in a signed message. This information is a much more reliable representation of the sender's identity than the **SMTP From** address.

Default security settings added to Global Address List

Including your group's default security settings in the Global Address List makes it easier to exchange encrypted e-mail messages within your organization. You add your group's security settings to the Global Address List by placing the certificate on your computer and then publishing it to the Global Address List. This feature is available on the **Security** tab in the **Options** dialog box (**Tools** menu).

Enabling Outlook 2000 SR-1 Features

You turn on the new security features in Outlook 2000 SR-1 by adding a setting to the Windows registry. You must first add a new subkey and value entry and then set its value; otherwise, the new features are not available.

To enable Outlook 2000 SR-1 security features:

1. In the Windows Registry Editor, select the following subkey:
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\9.0\Outlook
2. On the **Edit** menu, point to **New**, and click **Key**.
3. Enter the name **Security** for the new subkey and then select it.
4. On the **Edit** menu, point to **New**, and click **DWORD Value**.
5. Enter the name **EnableSRFeatures** for the new value and press **Enter**.
6. On the **Edit** menu, click **Modify** and then enter **1** in the **Value data** box and click **OK**.

If the value is set to **0**, the new security features are not enabled or visible to users.

You can use additional Windows registry settings to configure these security features, as described in the following section. The additional Windows registry entries are available only when you create the Security subkey and set value of **EnableSRFeatures** to **1**.

Configuring Outlook 2000 SR-1 Features

You can control many aspects of the new Outlook 200 SR-1 security features to properly configure messaging security and encryption for your organization's needs. To control these features, you specify settings in the Windows registry. For example, you can use Windows registry settings to require a security label on all outgoing mail or disable publishing to the Global Address List. These Windows registry entries are available when the **EnableSRFeatures** value is set, as described previously.

Note: A number of the new security registry settings have an equivalent setting on the **Security** tab in the **Options** dialog box (**Tools** menu). You can use the Windows registry to change these settings. However, setting the value in the user interface does not create or set the equivalent setting in the Windows registry.

The following table lists the Windows registry settings that you can add for your custom configuration. You add these value entries in the new HKEY_LOCAL_MACHINE\Software\Microsoft\Office\9.0\Outlook\Security subkey.

Value name	Value data (Data type)	Description	Corresponding UI option
EnableSRFeatures	0, 1 (DWORD)	Setting this value to 1 (or any non-zero value) enables Outlook 2000 SR-1 security features. Default is 0 .	None
AlwaysEncrypt	0, 1 (DWORD)	When you set the value to 1, all outgoing messages are encrypted. Default is 0 .	Encrypt contents check box
AlwaysSign	0, 1 (DWORD)	When you set the value to 1, all outgoing messages are signed. Default is 0 .	Add digital signature check box
ClearSign	0, 1 (DWORD)	When you set the value to 1, Clear Signed is used for all outgoing messages. Default is 0 .	Send clear text signed message check box
RequestSecureReceipt	0, 1 (DWORD)	When you set the value to 1, secure receipts are requested for all outgoing messages. Default is 0 .	Request secure receipt check box
ForceSecurityLabel	0, 1 (DWORD)	When you set this value to 1 , a label is required on all outgoing messages. (Note that the registry setting does not specify which label.) Default is 0 .	None
ForceSecurityLabelX	ASN encoded BLOB (Binary)	This value entry specifies whether a user-defined security label must be present on all outgoing signed messages. String can optionally include label, classification, and category. Default is no security label required.	None
SigStatusNoCRL	0, 1	Set to 0 means a missing	None

Value name	Value data (Data type)	Description	Corresponding UI option
	(DWORD)	CRL during signature validation is a warning. Set to 1 means a missing CRL is an error. Default is 0 .	
SigStatusNoTrustDecision	0, 1, 2 (DWORD)	Set to 0 means that a No Trust decision is allowed. Set to 1 means that a No Trust decision is a warning. Set to 2 means that a Not Trust decision is an error. Default is 0 .	None
PromoteErrorsAsWarnings	0, 1 (DWORD)	Set to 0 to promote Error Level 2 errors as errors. Set to 1 to promote Error Level 2 errors as warnings. Default is 0 .	None
PublishtoGalDisabled	0, 1 (DWORD)	Set to 1 to disable the Publish to GAL button. Default is 0 .	Publish to GAL button
FIPSMODE	0, 1 (DWORD)	Set to 1 to put Outlook into FIPS 140-1 mode. Default is 0 .	None
WarnAboutInvalid	0, 1, 2 (DWORD)	Set to 0 to display the Show and Ask check box (Secure E-mail Problem pont dialog box). Set to 1 to always show the dialog box. Set to 2 to never show the dialog box. Default is 2 .	Secure E-mail Problem pont dialog box
DisableContinueEncryption	0, 1, (DWORD)	Set to 0 to show the Continue Encrypting button on final Encryption Errors dialog box. Set to 1 to hide the button. Default is 0 .	Continue Encrypting button on final Encryption Errors dialog box
RespondtoReceiptRequest	0, 1, 2, 3 (DWORD)	Set to 0 to always send a receipt response and prompt for a password if needed. Set to 1 to prompt for a password when sending a receipt response. Set to 2 to never send a receipt response. Set to 3 to enforce sending a receipt response. Default is 0 .	None
NeedEncryptionString	String	Displays the specified string when the user tries unsuccessfully to open an	Default string

Value name	Value data (Data type)	Description	Corresponding UI option
		encrypted message. Can provide information about where to enroll in security. Default string is used unless value entry is set to another string.	

When you specify a value for **PromoteErrorsAsWarnings**, note that potential Error Level 2 conditions include the following:

- Unknown Signature Algorithm
- No Signing Certification Found
- Bad Attribute Sets
- No Issuer Cert found
- No CRL Found
- Out of Date CRL
- Root Trust Problem
- Out of Date CTL

The following table lists additional Windows registry settings that you can use for your custom configuration. These settings are contained in the HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\SMIME\SecurityPolicies\Default subkey.

Value name	Value data (Data type)	Description	Corresponding UI option
ShowWithMultiLabels	0, 1, (DWORD)	Set to 0 to attempt to display a message when the signature layer has different labels set in different signatures. Set to 1 to prevent display of message. Default is 0 .	None
CertErrorWithLabel	0, 1, 2 (DWORD)	Set to 0 to process a message with a certificate error when the message has a label. Set to 1 to deny access to a message with a certificate error. Set to 2 to ignore the message label and grant access to the message. (The user still sees a certificate error.) Default is 0 .	None

Additional Information

For more information about upgrading to Office 2000 SR-1, see “Deploying Office 2000 Service Release 1” in the Office Resource Kit Journal at <http://www.microsoft.com/office/ork>.

A discussion of MIME and a related protocol, PGP (Pretty Good Privacy) is included in S/MIME and OpenPGP at <http://www.imc.org/smime-pgpmime.html>.

Documents with details about the S/MIME standards include the following:

- S/MIME Version 3 Message Specification at <ftp://ftp.ietf.org/rfc/rfc2633.txt>.
- Cryptographic Message Syntax at <ftp://ftp.ietf.org/rfc/rfc2630.txt>.
- Enhanced Security Services for S/MIME at <ftp://ftp.ietf.org/rfc/rfc2634.txt>.